Security Plan

For

Student Financial Assistance

HR Modernization

Prepared by

SFA Modernization Partner

On

October 18, 2001

Version Number:	1.0
Originating Office:	SFA HR Department, HR Modernization System Security Officer, xx
Phone Number:	(202) xxx-xxxx

All HR Modernization documentation related to security is " Proprietary and Confidential" and will be marked as such. Distribution of HR Modernization security documentation to any individual or organization without a need-to-know is forbidden.
All draft versions of this security plan should be destroyed and the final version stored under restricted access.

HR Modernization Security Plan

`

1. System Identification

1.1. System Name/Title

Name: HR Modernization
Unique identifier: HR Platform
System Category: Major Application

1.2. Responsible Organization

United States Department of Education
Student Financial Aid (SFA)
Union Plaza Station
830 First St, NE
2nd Floor Room 22
Washington, DC 20002
(202) 377-3011

SFA has contracted with the Modernization Partner, Accenture, to develop HR Modernization and with Jamcracker, Inc., to host HR Modernization. Jamcracker corporate headquarters is located at:

Jamcracker, Inc.
19000 Homestead Rd.
Cupertino, CA 94015
(408) 725-4300

1.3. Information Contact(s)

The table below lists the HR Modernization contacts for SFA and the contractors, Accenture and Jamcracker, Inc.

Information Points of Contact			
	SFA	Accenture	Jamcracker
Name	Calvin Thomas	Scott Bone	Bruce Hartsough
Title	System Owner	Experienced Manager, HR Modernization	Vice President Engineering
Address	Union Center Plaza 830 First St, NE 2nd Floor Room 22 Washington DC 20002	One Freedom Square 11951 Freedom Drive Reston, VA 20190-5651	19000 Homestead Rd. Cupertino, CA 94015
Phone	(202) 377-3011	(703) 947-1236	(408) 725-4300
Email	calvin.thomas@ed.gov	scott.bone@accenture.com	bhartsough@jamcracker.com

1.4. Assignment of Security Responsibility

See Appendix 19 for a copy of the assignment letter for the position of SFA SSO.

Name	Role	Organization	Phone
Calvin Thomas	System Owner and Accreditation Official	SFA	(202) 377-3011
Scott Bone	System Manager and Certifying Official	Mod Partner	(703) 947-1236
xxxx	System Security Officer	SFA	(xxx) xxx-xxxx
Daniel J. Stahlnecker II	Director of Corporate Security	Jamcracker	(408) 725-4300
Stacy Roux	Quality Assurance Lead	Mod Partner	(202) 962-0860
Stacy Roux	Software Configuration Lead	Mod Partner	(202) 962-0860
Jamcracker Service Center (JSC)	Technical Support Representative	Mod Partner	(877) 848-2586
Ana Perez-Arrieta	HR Modernization Operations	Mod Partner	(202) 962-0859
Ana Perez-Arrieta	Training Lead	Mod Partner	(202) 962-0859
Allison Webster	Testing Lead	Mod Partner	(202) 962-0858

1.5. System Operation Status

HR Mod is a new SFA system under development. A small, live data pilot is scheduled to start on October 25, 2001. The Jamcracker Platform consists of three distinct operating environments that will take HR Mod into production, or as Jamcracker calls it, hot production:

- **Development:** The development environment is where Jamcracker engineers develop new versions of the Platform and is considered under constant change. This environment is only accessible by Jamcracker engineers and operations support staff.
- **Cold Production:** The cold production environment is the environment in which Jamcracker tests new software releases before releasing them to Hot Production. This environment is not available to customers and is considered under development.
- **Hot Production:** The hot production environment is the operational environment that Jamcracker customers access. This environment is the "live" environment and is considered operational.

1.6. General Description/Purpose

The HR Modernization vision was created to provide a framework for the rapid deployment of "best-of-breed" human resource and human capital Application Service Providers (ASPs) systems. HR Modernization utilizes an aggregator model (Jamcracker) to connect multiple ASPs. Users access individual applications through the aggregator using a single sign-on. The HR functional areas that will be integrated into the aggregator model include:

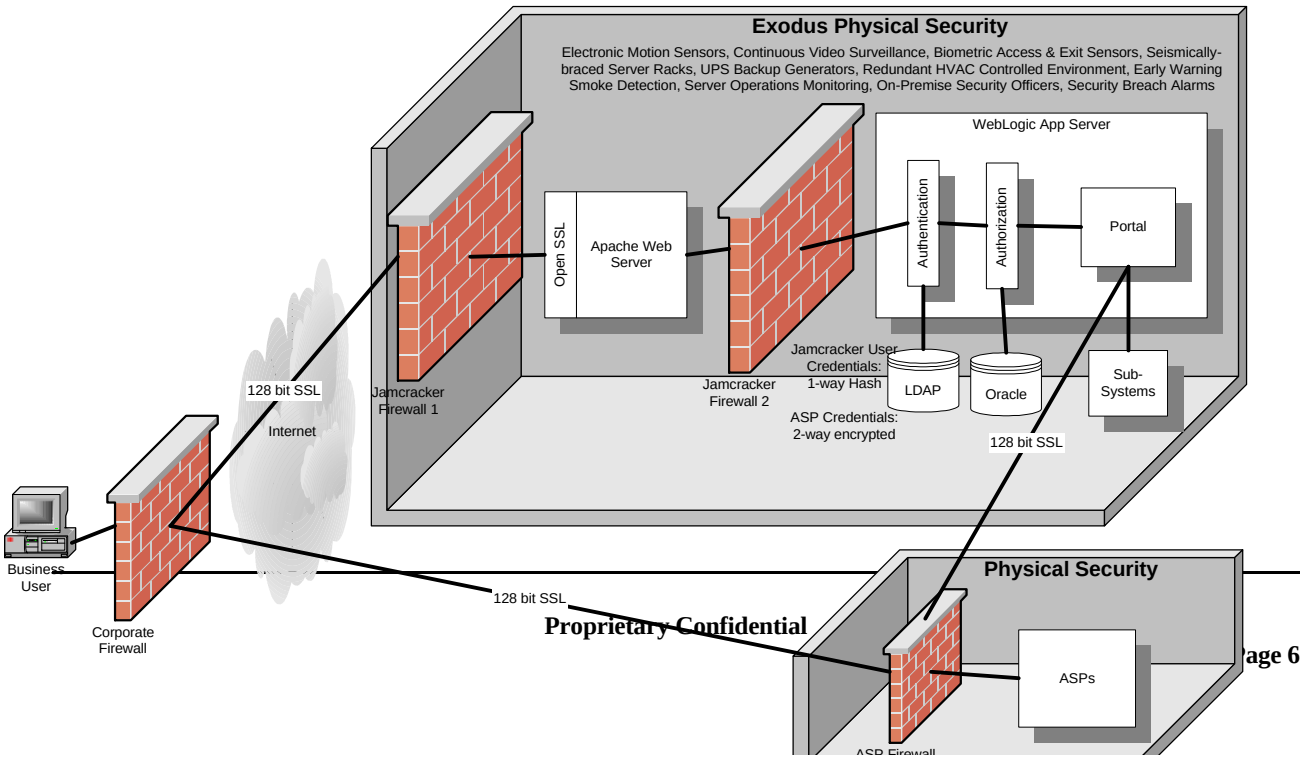
classification/recruiting/staffing, performance management, knowledge management, skill/career development and training, payroll administration and benefits administration.

Jamcracker's aggregator model is called Jamcracker Web Services Platform. The platform provides customers with a web interface for 3rd party application and ASP integration. The platform also provides the ability to support these 3rd party products via reporting, billing, and end-user provisioning capabilities. The Jamcracker Web Services Platform is hosted at an Exodus Communications Internet Data Center, located at Exodus SC8 Data Center, 500 Ironside Road, San Jose, CA.

Although the initial roll-out of HR Mod will only consist of Perform.com, a goal-setting and performance evaluation tool, it will eventually also include five other ASPs to be implemented in two separate roll-outs. All of these applications will be hosted by disparate commercial ASPs who will integrate onto the Jamcracker platform. The following table gives a description of the different SFA HR portals:

Portal	Description
Perform.com (Performance Management)	Goal setting, job reviews
Classification/Staffing/Recruiting	Job postings, job classification codes, resume submittal
Knowledge Management	Training information, HR policies and procedures, enterprise financial reports (FMS)
Benefits Administration	Available benefits, forms, online application for benefits
Skill/Career Development and Training	Training documentation, resources, career path info
Payroll Administration and Personnel Management	Pathway to FPPS for internal information transfer

For HR Mod, Jamcracker will control the access of users to the various human resource websites; the Jamcracker aggregator model will provide a single portal from which users will connects to the various ASPs. Essentially, an SFA user will log into the Jamcracker



website using his/her e-mail name as the user identification and a Jamcracker password. Once authentication is complete, Jamcracker will determine which areas of HR Mod the user is authorized access and show these options on the Jamcracker webpage. At that point, the user can choose which website to visit, and Jamcracker will redirect him/her to the new site and perform the log-in functions at the new site for the user. Users will then use the ASP's application to input and obtain data. No user information is kept at Jamcracker except for the authentication and authorization information; all SFA user application data is stored at the ASPs who host each HR application. See the table below for a break down of HR Mod users:

User Group	Description/Role (what user can do on HR Mod)	Means of Accessing HR Mod
SFA Employees	See Appendix 21	EDLAN or VDC
SFA Managers	See Appendix 21	EDLAN or VDC
SFA System Administrator	See Appendix 21	EDLAN or VDC
Jamcracker (break down into roles)	xx	Internal or some connection to Exodus data center?
Partner ASPs (break down into roles)	xx	40/128-bit SSL encryption and mutual authentication

1.7. System Environment

The system security boundaries for HR Mod encompass the Jamcracker production facility and the communication links between this facility and SFA employees, as well as to all associated ASPs.

All HR Mod system hardware and software as detailed below is located at the Exodus data center in San Jose, California. Exodus hosts all critical Jamcracker systems (see network diagram below). The Jamcracker headquarters building in Cupertino, California, contains the internal Jamcracker corporate LAN and has no relation to the system security of HR Mod.- *confirm- or is there a comm. connection between Jamcracker and Exodus on which HR Mod/platform work is performed (remote access)?What is that connection?*

Application Environment			
Service	**Application Used**	**Hardware Used**	**Software Used**
Application Servers	BEA WebLogic	Sun Ultra UNIX Servers	OS: Other:
Database Servers	Oracle Database	Sun Ultra UNIX Servers	OS: Other:
Authentication Servers	Netegrity Siteminder	Sun Ultra UNIX Servers	OS: Other:
Firewalls	Checkpoint Firewall-1/VPN1	Sun Ultra UNIX Servers	OS: Other:
WWW Servers	Apache	Sun Netra UNIX Servers	OS: Other:

Back-end equipment?			OS: Other:

The Jamcracker environment is a robust, redundant, multi-tiered network that is designed for maximum security and high availability. The network is comprised primarily of Sun Microsystems and Cisco Systems hardware and best-of-breed software providing the best service possible to the customers. In case of a full network operational failure, a cold production facility is available for automatic switchover after internal sensors have determined a catastrophic failure. Both hot and cold production sites are in the Exodus SC8 data center; Jamcracker is considering moving the cold production environment to a separate data center to create a more physically distributed environment.

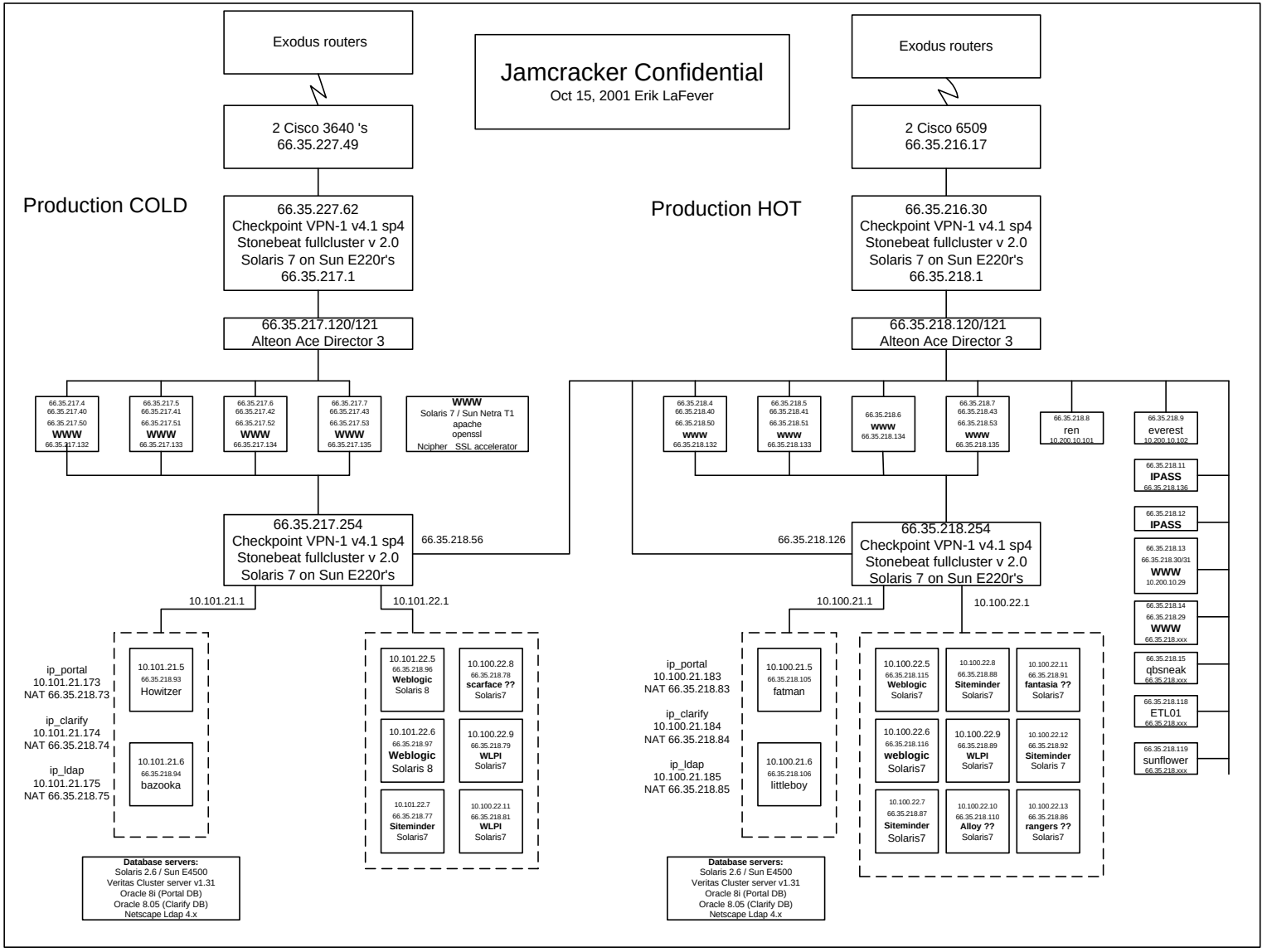
The perimeter of the Jamcracker network is protected by a Cisco 3640 with advanced ACLs to filter inbound connections and Checkpoint VPN-1 clustered firewalls for high availability and immediate fail-over capability. The Checkpoint firewall is configured to prevent all inbound connections except for those specifically authorized
.
Users obtain their services via web browsers and connect to one of four multi-homed web servers running Apache on Sun Microsystems Netra T1 servers, depending upon the load balancing calculations performed by an Alteon Ace Director. The Ace Director automatically routes the users' web requests to the web server that is capable of providing the fastest service. Additional hosts provide quality assurance testing locations used to run automated use case testing against the environment before new releases.

To protect the database servers from the rest of the network, another set of Checkpoint VPN-1 fullcluster firewalls are configured to only allow HTTP, SSL, and SSH traffic to move between the web servers and the application and database servers. Additionally, network address translation (NAT) is used to protect the true IP addresses of the systems. Oracle 8i is installed on a set of clustered Sun Enterprise 4500s. Additionally, back-end systems host products from Weblogic and Siteminder that provide analysis of ASP traffic and usage.

SFA users will most likely connect to Jamcracker over the Internet using either EDLan or the VDC as their Internet Service Provider, although users will be able to connect using any ISP from any location. Jamcracker's ASP partners can connect to the platform via remote SSL Internet access.

- communications resources—what is Jamcracker's internet connection? Any other comm. resources?
- Include any security software protecting the system and information—intrusion detection?

See a network diagram of Jamcracker components below.:



Jamcracker System Diagram

1.8. System Interconnection/Information Sharing

HR Mod only connects to the Internet; via the Internet, HR Mod is accessed by the systems described in the table below.

	System 1	System 2	System 3	System 4	Systems 5-?
Unique system ID	EDNET	VDC	Perform	N/A	Future ASPs that HR Mod connects to
Name of system	Dept of Education Network	Virtual Data Center	Perform	Internet	TBD
Organizations owning the other system	Dept of Education	SFA	Perform.com	N/A	TBD
Type of interconnection	via Internet	via Internet	via Internet	Jamcracker's ISP?	via Internet
System of Record if Privacy Act data is involved	N/A	N/A	N/A	N/A	TBD
Description of interaction among systems	Means by which SFA users connect to the Internet to then connect to HR Mod (Jamcracker)	Means by which SFA users connect to the Internet to then connect to HR Mod (Jamcracker)	Partner ASP that hosts employee performance application and is integrated to the Jamcracker platform	Means by which all users connect to HR Mod (Jamcracker)	TBD
Rules of behavior and controls that must be maintained by the interconnecting systems	See SFA's Rules of Behavior, Appendix 5	See SFA's Rules of Behavior, Appendix 5	See SLA between Jamcracker and SFA, Appendix 3, and guidelines in this section	N/A	See SLA between Jamcracker and SFA, Appendix 3, and guidelines in this section

The description that follows explains how HR Mod's connections from Jamcracker to all systems/users are protected. Included are security guidelines for all ASP partner contractors who require remote access to the Jamcracker platform. See Appendix 2 for a draft of the information Jamcracker plans to use to screen partner ASPs for security. See Appendix 3 for the SLA between Jamcracker and SFA, which is a flow-through SLA that applies to partner ASPs as well.

Jamcracker has built a robust security infrastructure to manage the integrity and confidentiality of data throughout the system—from the users in an enterprise's office (or on

the road), across the internet, to the servers and databases that store that information; whether they be at Jamcracker or at one of Jamcracker's ASP partners.

The following are some of the key components of Jamcracker's system:

Internet security: Jamcracker protects all connections to the Jamcracker Central workspace using Secure Socket Layer (SSL) protocol with 128-bit keys. This ensures that eavesdroppers cannot intercept critical information such as employees' user names and passwords. Jamcracker uses SSL, the industry standard for security browser-based communications.

Front-end authentication: Users of the system must authenticate at Jamcracker Central – Jamcracker's workspace and portal -- with their company name, user name, and password before they can access the system. Jamcracker uses industry-leading products to perform this authentication. Customers can define their own password policies such as minimum length, content guidelines, and expiration times.

In the future, Jamcracker will offer additional authentication mechanisms such as smart cards and biometric information.

Front-end access control: Users of the system can view only authorized content and services. Jamcracker uses industry leading applications to perform authorization checks to enforce this restriction.

Application access: Jamcracker provides a single sign-on solution, whereby users authenticate only once with Jamcracker to access all of their provisioned applications.

Jamcracker implements this solution using cryptographically secured tokens that comply with the Security Assertion Markup Language (SAML) specification. Using these tokens prevents theft of users' identities within the context of a given application, while single sign-on helps to eliminate security leaks caused by the difficulty of maintaining multiple passwords for each user.

Core services: A sophisticated workflow engine controls the core Jamcracker services of provisioning, customer relationship management (CRM), and system monitoring. The authorization mechanisms of Jamcracker's application server govern this engine's activities. This J2EE-compliant application server enforces a set of policies that, for instance, prevent one customer from accessing the billing records of another customer. Additional security measures are built into the databases so that errors in application code or policy creation do not inadvertently allow one customer to access another customer's data.

ASP connectivity: The connections between Jamcracker and its ASP partners are secured through the use of 40/128-bit SSL encryption and mutual authentication.

Criteria for Remote Access by Contractors

Specify security requirements and assess contractor capability.

1. Identify technology security requirements.
2. Identify security requirements that the contractor must meet in addition to those related to the specific technology.
3. Include all security requirements in the solicitation for outside bids.
4. Assess the contractor's capability to meet your security requirements.
5. Write the security requirements into the contract work statement. Include explicit procedures where necessary.
6. Execute a non-disclosure agreement if one is not already in place.

Determine contractor ability to comply with your organization's security policy.

1. Examine your organization's security policy and determine the applicability of each section to this contract.
2. Communicate your policy to your contractor.
3. Ensure that your contractor accepts your policy. Write this into the contract terms and conditions and/or contract work statement.
4. Require that your contractor demonstrate the ability to comply with your policy.

Require that the contractor software is installed and configured to operate securely.

1. Make any necessary preparations to receive the contractor software.
2. Document the contractor software configuration to be installed.
3. Create and record cryptographic checksums of the installed software.
4. Verify the authenticity of the software being installed.
5. Configure the contractor software to operate securely.
6. To the extent possible, ensure the contractor thoroughly tests their software in a non-production environment prior to moving the software into your operational systems.
7. If the installation must be performed remotely from your facility and network, ensure that all communications are performed securely.

Require that the contractor communicate securely with your site when operating remotely.

1. Authenticate the communicating hosts.
2. Authenticate the external (contractor) user.
3. Upon successful authentication, encrypt all subsequent communications between hosts and users for the exchange of sensitive information.
4. Document, monitor, and reset connection states.

Control contractor access to your systems.

When contractor processing can be explicitly scheduled

1. Require that the contractor notify you in advance when access is needed.
2. Require that the contractor describe exactly what actions will be taken when they access your system.

3. Analyze the impact of the task on other business-critical functions.
4. Allow contractor connectivity to your systems only when a scheduled task is to be performed. Disable access at other times.

When contractor processing must occur 24 hours a day or in an emergency

1. Establish pre-arranged procedures for 24-hour and emergency access as part of contract negotiations.

Look for unexpected changes to directories and files.

1. Establish priorities and schedules.
2. Maintain authoritative reference data for critical files and directories.
3. Verify the integrity of directories and files according to your established schedule.
4. Identify any missing files or directories.
5. Identify any new files and directories.
6. Investigate any unexpected changes among those you have identified.

Inspect your system and network logs.

1. Periodically inspect each type of log file.
2. Document any unusual entries that you discover.
3. Investigate each documented abnormality.
4. Report all confirmed evidences of intrusion (or attempted intrusion) to your organization's internal security point of contact.
5. Read security bulletins from trustworthy sources and other security publications regularly.

Review contractor performance.

For ongoing review

1. Establish a process for reviewing contractor compliance with specified security requirements.
2. Establish a process for reviewing contractor compliance with your security policy.
3. Conduct periodic reviews to verify contractor compliance.
4. Regularly execute a file system integrity-checking tool.
5. Ensure that no Trojan horses or viruses exist in the contractor software.
6. Review user problem reports.

For emergency access

1. Upon unscheduled or emergency access of your systems by the contractor, conduct an immediate review of pertinent logs if this is not performed automatically.
2. Perform a post-mortem review with the contractor to determine the cause of the emergency and discuss how to avoid this in the future.

1.9. Applicable Laws or Regulations Affecting the System

The following laws, regulations or policies establish requirements for confidentiality, integrity and availability for HR Mod.

Federal Laws

- Computer Security Act of 1987, Public Law 100-235, 101 Stat. 1724.
- Electronic Communications Privacy Act of 1986, Public Law 99-08, 100 Stat. 1848
- Fraud and Related Activity in connection with Access Devices and Computers, 5 United States Code 1029-1030,
- Freedom of Information Act, 5 United States Code 552, Public Law 93-502
- Privacy Act of 1974, 5 United States Code 552a, Public Law 99-08
- Security of Government Employees of 1950, United States Code 7501, Public Law 81-733
- Security Requirements for Government Employment of 1953, Executive Order 10450

Regulations

- OMB Circulars A-123, A-127, A-130
- National Security Decision Directive 145
- National Telecommunications Information System and Security Policy No. 2

Agency-Level

- Information Technology Security Policy of the Department of Education, Draft, May 2000
- SFA Security Policy, Draft, September 2001

The Privacy Act doesn't apply to HR Mod in its current configuration. As other HR application ASPs are added to the system, the Privacy Act may apply.

1.10. General Description of Information Sensitivity

The types of information stored in the Jamcracker Platform range in sensitivity from publicly available information such as customer company and employee names, to confidential information such as customer passwords and employee social security numbers. See Section 1.6 for the type of information involved in each planned HR Mod application.

As currently planned, the Perform application will handle SFA employee goal setting information. If this type of information is misused, corrupted or modified, the resulting risk is for SFA employee performance goals to become compromised or illicitly changed. SFA employees may lose trust in the application, resort to paper methods, and work in-person with supervisors to correct performance goals. If a future expansion of SFA's use of Perform introduces Privacy Act information and employee ratings, the risk level will increase. Also, as HR applications are added to HR Mod, different risks will ensue.

The sensitivity/criticality analysis focuses on the confidentiality, integrity, and availability requirements necessary for the different ASPs that will be associated with HR Mod. Each

was given a rating of Low, Medium, or High in each area, with the aggregate determining the system's overall rating.

Portal	Confidentiality	Integrity	Availability	Portal Status
Performance	Medium	Medium	Low	pilot Oct 2001
Recruiting	Low	Medium	Medium	planned
Career Devt	Low	Low	Low	planned
Benefits	Medium	High	Medium	planned
Knowledge Mgmt	Medium	Medium	Low	planned
HR Mod	**Medium**	**Medium/High**	**Medium/Low**	N/A

The most critical functionality for all of the different ASPs is to maintain the integrity of the data entered and stored within their databases, whether it be the goals that employees will be reviewed upon, the benefits available and requested by employees, or even the job postings for employment opportunities. Changes within that data, or an inability to tell if the data had been changed, would seriously compromise the capability of SFA to properly function in its support of its employees. Likewise, confidentiality is an important requirement due to sensitive information such as social security number, health records, and payroll records. Only in certain circumstances is availability a large issue, such as during the open period for benefits. In most other cases, however, loss of system availability, while inconvenient, would not seriously affect SFA's mission objectives, with (if necessary) paper records able to replace electronic during the down period.

2. Management Controls

2.1. Risk Assessment and Management

Risk levels associated with the Jamcracker Platform are assessed on a monthly basis. This assessment covers 25 different threats to the platform in 6 specific categories. Those categories include:

- Passive Attacks
- Active Attacks
- Close-In Attacks
- Insider Attacks
- Non-malicious Attacks
- Distribution Attacks

By adopting a more rapid internal assessment strategy Jamcracker is able to evaluate new risks to the environment faster and realign security expenditures to face new risks and determine the impact of new security measures over time.

2.2. Review of Security Controls

Jamcracker has contracted Internet Security Systems to perform annual penetration tests on the Jamcracker Platform. This level of testing will allow Jamcracker to validate the

assessments performed by the internal security operations team. The first test by Internet Security Systems in scheduled for Q2/2002.

Jamcracker has also contracted Arca Systems to perform a security analysis of the Jamcracker Platform source code. The recommendations from Arca systems are then incorporated into future releases of the Jamcracker Platform. The first Arca Systems assessment was conducted in Q2/2000 (findings and actions taken) and a second test will be scheduled for Q1/2002. Besides Jamcracker's scheduled penetration tests and source code analysis, KPMG Consulting is conducting an independent risk assessment of HR Mod during October 2001.

2.3. Rules of Behavior

Jamcracker requires all employees to read and sign the System User Security Policy Agreement when they are hired. Jamcracker system administrators are further required to read and sign the System Administrator Security Policy Agreement before they can perform administrative operations within the Jamcracker Platform. See Appendix 4 for these agreements. See Appendix 6 for Jamcracker's Internet Usage Policy and Appendix 18 for Acceptable Usage Guidelines.

SFA users are required to…read and sign HR Mod Rules of Behavior…see Appendix 5.

2.4. Planning for Security in the Life Cycle

HR Mod is in the Implementation Phase and will enter the operational phase when the pilot of the first human resources application, Perform, goes lives at the end of October 2001. After Perform expands beyond pilot operations into full implementation, the other human resources application that will be added to HR Mod will start to enter the development life cycle.

2.4.1. Initiation Phase

As new features are added to the Jamcracker Platform security considerations are documented in the Functional Requirements Document (FRD) for that feature. This document specifies the general customer requirements of the feature as well as any security requirements associated with its implementation such as requirements that the data handled by the feature be encrypted or the auditing levels required in order to properly assess the use of the feature.

See Section 1.10 for the sensitivity assessment the customer, SFA/Modernization Partner conducted to help understand how HR Mod data needs protection. As new applications are added to HR Mod, sensitivity assessments will be conducted for each application to help develop requirements.

2.4.2. Development/Acquisition Phase

After the FRD is complete it is transitioned to the engineering/development team where the requested functionality is coded and prepared for integration into the workspace. Before the feature is implemented into the Platform it undergoes a rigorous quality assurance process in which all functionality is tested. Jamcracker security product managers will also QA the required security functionality before the feature is deemed ready for production.

Before the procurement action, SFA did not develop a formal list of appropriate security controls and associated evaluation and test procedures. However, SFA performed due diligence in reviewing Jamcracker's platform to include how they secured their operations. Along the way, security requirements could be updated if new threats/vulnerabilities were identified and/or if new technologies were implemented.

As part of the Software Evaluation Process, Jamcracker and Perform.com were both assessed in the following security areas:

- Password protection and policies
- Data Usage and Privacy rules
- SSL 128 bit data encryption standards
- Disaster/Recovery procedures
- Data backup procedures
- Internal and External Security policies and procedures
- Data storage and archiving procedures
- Technical Architecture and firewalls
- Network topology
- Use of cookies
- Use of clients
- SLA's

Additionally, Jamcracker and Perform.com were rigorous tested through a comprehensive testing model developed specifically for netsourced applications at SFA. Test Scripts, Test Data and Expected Results were developed for each phase of testing except for Performance/Scalability testing, where results were provided by an independent Performance and Scalability test of the Jamcracker Platform. The testing methodology includes the following phases:

- Integration Validation testing of Perform.com onto the Jamcracker Platform
- Full Product Test of every function in both applications
- Full Capability Release Test
- Operational Readiness Test
- Performance/Scalability Testing
- Deployment Verification Testing

2.4.3. Implementation Phase

Once the features code has been approved it is transitioned to the Jamcracker Production Operations Team, which will integrate the feature into Jamcracker's Cold Production environment for further testing and analysis. Further security testing will be performed in order to assess the impact of the new code in the Cold Production environment. If any issues are discovered the code will be returned to the engineering/development team for further QA testing and revised. See Appendix 20 for Jamcracker's change management manual. All system tests are documented, and as mentioned in section 2.4.6, the system is technically evaluated before release into hot production. Jamcracker approved HR Mod for hot production on September 29, 2001.

2.4.4. Operation/Maintenance Phase

After the new feature is deemed production ready the code is installed via a software patch during a scheduled maintenance window by Jamcracker's Production Operations team. The new feature is then considered "live." If there are any issues discovered in the code after it goes "live" a trouble ticket is opened by the Jamcracker Support Center and passed to the engineering/development team for resolution and the process restarts from section 2.4.2 Development Acquisition Phase.

2.4.5. Disposal Phase

The only time information is purged from the system is when specific customer events occur. These events include when a customer discontinues the Jamcracker service or when an employee leaves a customer company. When an event such as those described above occurs, the related customer records are purged from the database. Due to service level agreements, the customer's data may still be retained on a backup medium in the event that the customer requires access to the data at a later date.

- How is customer data that is maintained for future access backed up? What controls ensure the confidentiality of this saved data (is sensitive data encrypted)?
- How are customer records purged from the system? (overwritten, degaussed or destroyed, etc.)

2.4.6. Authorize Processing

HR Mod will request authorization to process on October x, 2001. The head of SFA's HR Department is the management official responsible for deciding whether to authorize processing. From Jamcracker's end, the Director of Release Operations has the final approval on all new features and new software releases moved into Hot Production.

Director of Release Operations
Steve Pool
Jamcracker, Inc.
19000 Homestead Rd.
Cupertino, CA 94015
(408)725 4300

3. Operational Controls

3.1. Personnel Security

Personnel Screening
Verification checks on permanent staff are carried out at the time of job applications. This should include the following controls:

- Availability of satisfactory character references, e.g. one business and one personal
- A check (for completeness and accuracy) of the applicant's curriculum vitae
- Confirmation of claimed academic and professional qualifications
- Independent identity checks (passport or similar document).

Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities, and in particular if these are handling sensitive information, e.g., financial information or highly confidential information, the organization will also carry out a credit check. For staff holding positions of considerable authority this check should be repeated periodically.

A similar screening process will be carried out for contractors and temporary staff. If staff is provided through an agency, the contract with the agency should clearly specify the agency's responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern.

Confidentiality Agreements
Confidentiality or non-disclosure agreements are used to give notice that information is confidential or secret. Employees should normally sign such an agreement as part of their initial terms and conditions of employment.

Casual staff and third party users not already covered by an existing contract (containing the confidentiality agreement) should be required to sign a confidentiality agreement prior to being given access to information processing facilities.

Confidentiality agreements should be reviewed when there are changes to terms of employment or contract, particularly when employees are due to leave the organization or contracts are due to end.

As Jamcracker's Corporate IT Security Policy states, all employees must comply with the Information Security Policies that exist at Jamcracker. Any information security incident that is the result of non-compliance with the policies will result in immediate disciplinary action up to and including termination. See Appendix 7 for friendly and unfriendly termination procedures.

Jamcracker adheres to a separation of duties policy between departments, and limits users with "root" access privileges to reduce threats from internal misuse; user access is restricted

to the minimum necessary to perform the job. Jamcracker has established procedures for requesting, establishing, issuing, and closing user accounts (see Appendix 14 Platform Security Platform Requirements).

- Have all positions been reviewed for sensitivity level? Insert chart of personnel sensitivity level or confirm

3.2. Physical and Environment Protection

The Jamcracker Web Services Platform is hosted at an Exodus Communications Internet Data Center San Jose, California. This data center provides a high level of security and fault tolerance. Exodus communications handles physical security at their facilities. The Exodus data center has the following security systems in place to protect Jamcracker:

- Electronic Motion Sensors
- Continuous Video Surveillance (building-wide)
- Biometric Access and Exit Sensors to data center
- Seismically Braced Server Racks
- UPS and Backup Generators
- Redundant HVAC Controls for data center
- Early Warning Smoke Detectors
- 27/7/365 Systems Monitoring of computer and environmental systems
- On Premises Security Officers
- Security Breach Alarms for building and data center
- plumbing leaks precautions?

The biometric access system to the data center retains an event log and has a backup power supply which will permit personnel to leave in the event all power systems fail. No mobile/portable systems support the Jamcracker Platform so theft prevention in this area is not a concern. While all customer communications and communications between sites is encrypted using either SSL or 3DES VPNs, physical interception of this encrypted data is prevented by xxxxx.

What are building access procedures at Exodus vs. the data center (biometric)?

Physical security at Jamcracker corporate headquarters is provided by Pinkerton Security services. Security guards man the headquarters 24/7/365, including after hours patrols of the interior, exterior, and parking lot. Security guards ensure all employees entering the building wear photo ID badges and that visitors sign in and are badged. The guards have established procedures for handling emergencies (fire, chemical, bomb threat, evacuation, etc.). All alarmed doors report to a central system.

All recipients of building photo ID cards are required to sign for the card at the time of issuance and are required to be returned upon termination. A list of all issued photo ID cards

is maintained and there is a set procedure for reporting stolen badges. Employees do challenge and escort strangers to their stated destinations, and unguarded emergency exits are locked to outside entry to prevent unauthorized access. Depending on location, ground, first and second floor windows are barred, screened or shatter-proof.

3.3. Production, Input/Output Controls

The process for adding new features to the platform is described in Section 2.4 Planning for Security in the Lifecycle. See Appendix 11 for Jamcracker incident response procedures. See Appendix 8 for Jamcracker's Data Classification Guidelines which describe four levels of data sensitivity and the corresponding procedures for storage, transmission and destruction. A brief summary of controls is described here. See Appendix 9 for Jamcracker Guidelines for Encryption of Data, and Appendix 10 for their Pretty Good Privacy Usage Guidelines. Jamcracker has a help desk to provide advice and help respond to security incidents in a timely manner.

Labeling
Clear and appropriate, as per the data classification, labeling must be applied to all information, data and documents so that all users are aware of the ownership and the classification of the information. For example, a document's security classification level and ownership should be indicated in the header and footer on each page of the document.

Media handling and security
Any person required to use removable media such as diskettes must be explicitly authorized to do so. Removable media must be handled in a very cautious way as not to compromise the confidentiality of the organization's data. It is thus a requirement to consider the classification of the data that is copied onto removable media and handle it accordingly. Data encryption must be considered and used when available.

Data Exchange
Internal, confidential or secret data and information may only be transferred across networks or copied to external media when the confidentiality and integrity can be assured by means of encryption and digital signature. The same type of information may only be sent by fax when more secure methods are not possible. The owner and the recipient of the information must both formally agree on this type of transmission beforehand.

- Procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media
- Audit trails for receipt of sensitive inputs/outputs
- Procedures for restricting access to output products
- Procedures and controls used for transporting or mailing media or printed output
- Audit trails for inventory management
- Media storage vault or library-physical, environmental protection controls/procedures

- Procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse
- Procedures for shredding or other destructive measures for hardcopy media when no longer required

3.4. Contingency Planning

All contingency and disaster recover plans are covered in the Jamcracker Disaster Recovery Plan, which can be found in Appendix 12, a separate self-contained document.

3.5. Application Software Maintenance Controls

HR Mod software is fully developed under contract with Jamcracker; SFA doesn't own the software or maintain copies but rather relies on Jamcracker and its ASP partners to provide the HR Mod services that SFA users will access via the Internet. The Jamcracker Workspace Platform is owned by Jamcracker, Inc., and has been developed to be used through the Internet by Jamcracker customers. There is a formal change control procedure in place for making changes to the Platform. This process is highlighted in Section 2.4. All changes to application software are documented and there are procedures to handle emergency fixes. See Appendix 20 for Jamcracker's Change Administration and Rollout Management Manual. [get softcopy?]

All engineering/development related application testing is performed on generic non-production related data. This ensures that access to sensitive customer data is limited to those Jamcracker employees with "need to know" access.

3.6. Data Integrity/Validation Controls

A draft copy of Jamcracker's Data Integrity Policy can be found in Appendix 13.
Jamcracker uses a wide variety of tools to ensure data integrity and the integrity of validation controls. They include:

- 3rd party security audits on both system infrastructures, system log files, and Platform source code (Internet Security Systems will be performing annual penetration tests on the Jamcracker Platform starting Q2/2002)
- Monthly internal Platform audits by Jamcracker's Security Operations Team
- Security Assessments tools, i.e. system vulnerability scanners, password crackers, and custom scripts
- Systems and Network Performance tools, i.e. HP OpenView and NAI Network Sniffers.
- Input validation on critical fields within the Jamcracker Platform to find errors and omissions. All data fields used in critical process functions are format specific and won't be accepted if the data doesn't match the format.
- *Are reconciliation routines used by the system, i.e., checksums, hash totals, record counts? Include a description of the actions taken to resolve any discrepancies.*

- *Is integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions?*
- *Are intrusion detection tools installed on the system?*
- *Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?* Is this answered by the bullet stating "3rd party security audits on both system infrastructure, system log files…" Is it real-time monitoring?

3.7. Documentation

Documentation for the daily operation of the Jamcracker Workspace Platform is contained within the Platform Run Books. These documents include instructions for general system maintenance procedures, troubleshooting and support procedures, and data backup and recovery procedures. These documents are updated on a regular basis to reflect changes within the Platform and new security processes that are implemented during the product lifecycle.

Documentation that may not be used as frequently for daily operations like the disaster recovery plan, user security agreements, change management manual, corporate IT security policy, etc., are also maintained at Jamcracker.

- Do you maintain (please confirm):
  - vendor documentation of hardware/software (if you use any vendors)
  - functional requirements
  - security plan
  - test results documents
  - emergency procedures
  - risk assessment
  - certification/accreditation statements/documents
  - verification reviews/site inspections

3.8. Security Awareness Training

SFA User Training

The Modernization Partner will provide training to SFA users on the Jamcracker platform and Perform.com, the first HR application deployed. To facilitate this training, Jamcracker has trained eight Modernization Partner personnel on the platform and provided an instructional designer to help work with Jamcracker training materials.

The training will be performance-based, to ensure that SFA employees know how to complete the basic functions using the new application, and not designed only to provide

process information. This means that the training will maximize employee involvement and minimize passive listening or reading and include activities that focus on performing the most frequent, routine skills. Infrequent activities will be supported by the User Training and Reference Guide.

SFA will utilize a "Train-the-Trainer" model, where super users will be developed to perform training throughout the organization, as well as provide a superior level support during production. These trainers will be instructed on the best techniques for instructing and facilitating sessions with users, as well as receive a comprehensive training on the Jamcracker platform and Perform.com.

All training developed will be modular, so that various modules can be combined or separated to address additional training needs of specific audience groups. It is anticipated that additional training or coaching may be required after implementation to reinforce skills.

The Primary Training deliverables for SFA include:

The **SFA Employee Training Presentation** summarizes the key information that must be conveyed to all users. Such information will include an overview of the new Performance Development Process steps and walkthrough of basic functionality and processes using Perform.com. Additionally, a communication plan for the organization will be developed that includes timed communication announcements, posters, smart cards and job aids.

The **Training Scenarios** provide SFA employees with the opportunity to "practice" what they have learned while in the risk-free training environment. This will help build employee's confidence that they will be able to execute what they learned on their own. Absorption of knowledge rates will be measured to ensure that those employees who needed additional practice with the new system are provided that opportunity.

The **User Training and Reference Guide** assists SFA employees during the training session and when back at their desks executing the steps of the process. The Training and Reference Guide will provide a detailed overview of the new Performance Development Process intent and steps, rationale for the selection of Perform.com, and step-by-step instructions for all the functions employees are able to complete through Perform.com

The **Facilitator Guide** provides support/instruction for the Trainers delivering the session. The Facilitator Guide will contain information including facilitation skills, session overview, process overview, application training and role awareness.

The **Administrator Supplementary Reference Guide** will be distributed only to application administrators within the SFA HR organization. The Administrator Guide will provide step-by-step procedures for the completion of administrative duties including user set-up, addition of a competency, report generation, etc.

Jamcracker User Training

All employees of the organization, and, where relevant, third party users, should receive appropriate training and regular updates in organizational policies and procedures. This includes security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities (e.g., log-on procedure, use of software packages) before access to information or services is granted.

Users who are not proficient in the use of the application programs are required to enroll in appropriate training classes offered through the Educational Services Department in cooperation with the Technology Operations Team. The Technology Operations Team shall hold regular training classes on the management of microcomputer disks. This training shall include a discussion of strategies available to avoid data loss, including proper operating system command usage, backup strategies, and virus detection.

4. Technical Controls

4.1. Identification and Authentication

The technical controls surrounding the Jamcracker Platform are designed to be customer configurable. That allows each customer to choose the level of security they feel most comfortable with. The details of the technical controls implemented within the Jamcracker Workspace can be found in the Jamcracker Platform Security Requirements document (Appendix 14). Policies and procedures for changing passwords for Jamcracker systems personnel and ASP partner personnel are described in Appendix 16. Jamcracker Guidelines for Secure Password Selection are found in Appendix 15.

HR Modernization will use SFA e-mail identifiers as userid's, and will require passwords with a minimum length of six characters and a maximum length of twenty, with one character required to be of a different capitalization, and one to be numeric. SFA user passwords will be changed every 30 days, but will have a limit of three password changes per session to prevent password cycling to original passwords. No passwords may be repeated

4.2. Logical Access Controls

See Jamcracker Platform Security Requirements document (Appendix 14). HR Mod-specific.

4.3. Public Access Controls

HR Mod (the Jamcracker Workspace Platform) is not available to the general public.

4.4. Audit Trails

The Jamcracker Platform captures audit trails from many devices. Those devices include:

- Firewalls

- Authentication Servers
- LDAP Servers
- Database Servers
- Application Servers
- Web Servers

All audit trails are stored on a secure logging server accessible only to the Jamcracker Security Operations team and Vinciti, Jamcracker's log analysis server partner. Access to the audit logs is available in a read-only format to Jamcracker's Engineering and Developments for troubleshooting purposes. All audit logs are stored on magnetic tape for archive purposes, and the tapes are retained for 90 days. See Appendix 17 for a description of Jamcracker's auditing functions.

Due to the fact that Jamcracker captures auditing data from many devices, time synchronization of log entries is critical. To accomplish this, Jamcracker uses a network time server that supports redundant GPS, ACTS, and NTP time references.

- Is the confidentiality of audit trail information protected if, for examples, it records personal information about users?
- Describe how frequently audit trails are reviewed

5. Appendices

5.1. Appendix 1 – Jamcracker Corporate IT Security Policy

See separate file.

5.2. Appendix 2 – Security Screening for Partner ASPs

Security for Jamcracker Information Technology Service Contracts
(Draft Outline)

Specify security requirements and assess contractor capability.

1. Identify technology security requirements.
2. Identify security requirements that the contractor must meet in addition to those related to the specific technology.
3. Include all security requirements in the solicitation for outside bids.
4. Assess the contractor's capability to meet your security requirements.
5. Write the security requirements into the contract work statement. Include explicit procedures where necessary.
6. Execute a non-disclosure agreement if one is not already in place.

Determine contractor ability to comply with your organization's security policy.

1. Examine your organization's security policy and determine the applicability of each section to this contract.
2. Communicate your policy to your contractor.
3. Ensure that your contractor accepts your policy. Write this into the contract terms and conditions and/or contract work statement.
4. Require that your contractor demonstrate the ability to comply with your policy.

Require that the contractor software is installed and configured to operate securely.

1. Make any necessary preparations to receive the contractor software.
2. Document the contractor software configuration to be installed.
3. Create and record cryptographic checksums of the installed software.
4. Verify the authenticity of the software being installed.
5. Configure the contractor software to operate securely.
6. To the extent possible, ensure the contractor thoroughly tests their software in a non-production environment prior to moving the software into your operational systems.
7. If the installation must be performed remotely from your facility and network, ensure that all communications are performed securely.

Require that the contractor communicate securely with your site when operating remotely.

1. Authenticate the communicating hosts.
2. Authenticate the external (contractor) user.
3. Upon successful authentication, encrypt all subsequent communications between hosts and users for the exchange of sensitive information.
4. Document, monitor, and reset connection states.

Control contractor access to your systems.

When contractor processing can be explicitly scheduled

1. Require that the contractor notify you in advance when access is needed.
2. Require that the contractor describe exactly what actions will be taken when they access your system.
3. Analyze the impact of the task on other business-critical functions.
4. Allow contractor connectivity to your systems only when a scheduled task is to be performed. Disable access at other times.

When contractor processing must occur 24 hours a day or in an emergency

1. Establish pre-arranged procedures for 24-hour and emergency access as part of contract negotiations.

Look for unexpected changes to directories and files.

1. Establish priorities and schedules.
2. Maintain authoritative reference data for critical files and directories.
3. Verify the integrity of directories and files according to your established schedule.
4. Identify any missing files or directories.
5. Identify any new files and directories.
6. Investigate any unexpected changes among those you have identified.

Inspect your system and network logs.

1. Periodically inspect each type of log file.
2. Document any unusual entries that you discover.
3. Investigate each documented abnormality.
4. Report all confirmed evidences of intrusion (or attempted intrusion) to your organization’s internal security point of contact.
5. Read security bulletins from trustworthy sources and other security publications regularly.

Review contractor performance.

For ongoing review

1. Establish a process for reviewing contractor compliance with specified security requirements.
2. Establish a process for reviewing contractor compliance with your security policy.
3. Conduct periodic reviews to verify contractor compliance.
4. Regularly execute a file system integrity-checking tool.
5. Ensure that no Trojan horses or viruses exist in the contractor software.
6. Review user problem reports.

For emergency access

1. Upon unscheduled or emergency access of your systems by the contractor, conduct an immediate review of pertinent logs if this is not performed automatically.
2. Perform a post-mortem review with the contractor to determine the cause of the emergency and discuss how to avoid this in the future.

5.3. Appendix 3 – SLA between Jamcracker and SFA

Service Level Agreement

Contractor agrees to adhere to the levels of service outlined below with respect to the Jamcracker Service Center ("JSC")* and Jamcracker Central (collectively, the "Services") and other Jamcracker Services accepted and in use by SFA ("Other Services"). Contractor through its service provider will use commercially reasonable efforts to enforce industry standards for network, data and physical site security in order to protect the privacy and confidentiality of the SFA's data and to prevent access to such data by unauthorized users with respect to the Services and Other Services.

1. Availability of the JSC and Jamcracker Central.

1.1 Contractor through its service provider will offer and maintain personnel with technical, operations and management skills necessary to support the JSC 24 hours per day, 7 days a week.

1.2 Contractor through its service provider will monitor the JSC and Jamcracker Central 24 hours per day, 7 days a week.

1.3 The JSC will be available to SFA by telephone and SFA's email and Jamcracker Central will be available to SFA by e-mail (via Jamcracker Central) and real-time Internet chat. Support will be provided in English only.

2. Service Level Commitments.

2.1 *JSC.* The JSC will contact SFA to address SFA's service request (whether received by telephone, email, trouble ticket or Internet chat) within 120 seconds of receipt for ninety percent (90%) of all requests, measured monthly, excluding the time required for

transmittal of the response to or from the JSC (the "Response Time Commitment"), or SFA will be entitled to receive the credit described in Section 2.5, below, to be applied to SFA's invoice for the month following any month in which such Response Time Commitment is not attained, excluding unavailability caused by the following:

(a) Scheduled down-time for maintenance and upgrades, provided SFA is given at least 3 days' notice of such maintenance;

(b) Failures in the larger telecommunications network, including failures that are outside Contractor's and its service provider's control or the control of its telecommunications provider;

(c) Hardware or software problems of SFA that prevent/disrupt access;

(d) Emergency maintenance deemed necessary by Contractor's service provider to maintain the integrity, security or performance of the telecommunications system.

(e) The discontinuation of any Service for reasons outside its reasonable control.,

2.2 *Jamcracker Central*. Contractor agrees that Jamcracker Central will meet or exceed 99.5% availability (the "Jamcracker Central Up-Time Commitment"), measured monthly.

2.3 *Other Services.* Contractor agrees that Other Services will meet or exceed 95.0% availability between 6:00 am and 9:00 pm Pacific Time, Monday through Friday (the "Other Services Up-Time Commitment"), measured monthly. The Jamcracker Central Up-time Commitment and the Other Services Up-Time Commitment are collectively referred to herein as the "Up-Time Commitments."

2.4 The Up-Time Commitments exclude unavailability caused by the following:

(a) Scheduled down-time for maintenance and upgrades. The current maintenance window is between 12:01 am and 3:00 am every Sunday morning, Pacific Time for Jamcracker Central. This maintenance window is subject to change with notice to SFA;

(b) Failures in the larger Internet network, including failures that are outside Contractor's and its service provider's control or the control of its hosting and network provider;

(c) Failures, availability drops, or availability degradation due to causes beyond Contractor's and its service provider's direct control;

(d) Hardware or software problems of SFA that prevent/disrupt access;

(f) Emergency maintenance deemed necessary by Contractor's service provider to maintain the integrity or performance of the network.

(g) The discontinuation of any Service for reasons outside its reasonable control.,

2.5 If Contractor through its service provider fails to meet the Response Time Commitment or the Up-Time Commitments (collectively, the "Service Level Commitments") described in Section 2 during any given month, then SFA shall be entitled to receive a credit equal to twenty-five percent (25%) of the fees paid by SFA for the JSC, with respect to the Response Time Commitment, for Jamcracker Central, with respect to the Jamcracker Central Up-Time Commitment, or for any applicable Other Services, with respect to the Other Services Up-Time Commitment, for the month in which any such failure occurs (the "Credit"), with such Credit to be applied to SFA's account for the month following the month in which the applicable Service Level Commitment was not met.

2.6 To be eligible to receive the Credit, SFA must notify Contractor's service provider of any down-time within 24 hours of experiencing the disruption of service, via given via email to SLA@jamcracker.com, or, if email is not available, by telephone call to the JSC. Contractor's service provider will acknowledge receipt of the complaint within 72 business hours of receipt.

2.7 In the event of the discontinuation of any Service or Other Service for reasons outside Contractor's or its service provider's reasonable control, Contractor will give SFA at least thirty (30) days' notice of such discontinuation, or less if Contractor has less notice or is prohibited for confidentiality reasons from providing such notice. Contractor further agrees that if SFA may obtain such discontinued Service or Other Service or a similar, comparable or replacement service directly from an alternative service provider, Contractor will assist SFA in doing so. Contractor reserves the right to reasonably modify the categories, features, and functionality of the Services or Other Services to the extent required by its service provider's licensors at any time without notice, but will use reasonable efforts to give a 30-day notice to SFA regarding modifications to the Services or Other Services.

3. Case Resolution.

3.1 Levels of Severity

Cases shall be categorized according to the following levels of severity:

(a) Priority 1 cases are cases in which the JSC, Jamcracker Central or the Other Services are not functioning or available to SFA.

(b) Priority 2 cases are cases in which a significant functionality or feature of the JSC, Jamcracker Central or the Other Services is materially unavailable.

(c) Priority 3 cases are all other cases concerning the JSC, Jamcracker Central or the Other Services.

3.2 Resource Allocation and Updates

For all cases, Contractor through its service provider will assign the appropriate resources to resolve the case in an expedient manner. For Priority 1 cases, Contractor's service provider will update SFA 4 times daily regarding the status, plans and estimated time for resolution. For Priority 2 and 3 cases, Contractor's service provider will update SFA twice and once, respectively, daily regarding the

status, plans and estimated time for resolution. The updates can be provided more or less often if customer so requests.

3.3 Escalation

The JSC will contact Contractor, or other information technology representative designated by SFA, or the SFA requesting support within fifteen (15) minutes of determining that SFA's support case cannot not be resolved remotely by Contractor's service provider, but must be resolved on-site. Contractor's service provider has 7x24 support and case escalation procedures with respect to each of its service providers for the resolution of issues requiring technical support from the provider of Other Services.

If unusual circumstances require escalation, SFA may follow the following escalation procedures, in order:

(a) Contact the JSC at 1-408-725-4300 and ask to speak to the shift lead.

(b) Contact the JSC manager, through the JSC, via mobile phone or via pager, or, alternatively, contact the Technical Account Manager assigned to SFA. The names and contact numbers will be provided to SFA at the time of services deployment.

(c) Contact the Vice President of Customer Care via mobile phone or via pager at contact numbers to be provided.

4. Recourse.

SFA may terminate the Services without penalty if Contractor through its service providers fails to meet or exceed the Service Level Commitments or other commitments in this Service Levels Agreement for two (2) months in any twelve (12) month period. Except for the right to terminate described in the preceding sentence, Contractor's entire liability for its failure to meet any of the obligations described in this Service Levels Agreement shall be limited to the Credit to be applied to SFA's account for the month following the month in which the applicable Service Level Commitment was not met.

*Contractor's service provider's toll-free number may be accessed by users in the US only. Users outside the US may access the JSC by calling (602) 282-8400.

5.4. Appendix 4 – Jamcracker User Agreements/Rules of Behavior

System Users Security Policy Agreement

This is a legal agreement between you and Jamcracker Inc, a Delaware corporation having an address of 19000 Homestead Road, Cupertino, CA 95014. By signing this agreement, you are agreeing to be bound by the terms of this agreement. If you refuse to sign this agreement you will be denied access to the Jamcracker network at the User level.

Purpose

As a system user of Jamcracker, you will have access to company resources that are sensitive. With the privilege of systems access also comes a responsibility to conduct yourself in a manner deemed appropriate by Jamcracker Inc.

Termination

This agreement will remain in effect until Jamcracker Inc. or you have terminated your employment with Jamcracker.

Conduct

You agree that at all times you shall conduct yourself in compliance with all applicable Jamcracker policies, federal and local laws and regulations, including, without limitation laws regulating your professional status and designation. You further agree to the following:

- The system is to be maintained within the guidelines specified by the corporate Information Technology and Information Systems Security policies.
- No modifications to any system security policies, including logging will be made.
- The password on the local Administrator account will not change.
- The local Administrator account will not be disabled.
- Group membership on the system will not be modified.
- No operating systems or applications, which have not been authorized in accordance with the corporate policy, will be installed.

Agreement

I _____ fully understand my responsibilities and duties as a Jamcracker system user as defined by this agreement and the Jamcracker Information Systems Security Policy. I shall conduct myself ethically and not abuse my position as a system user. I understand that any violation of this agreement or any other company policies can be the basis for disciplinary action up to and including termination or judicial action.

_____ _____

User Signature *Security Representative Signature*

Date: _____ Date: _____

System Administrator Security Policy Agreement

This is a legal agreement between you and Jamcracker, a Delaware corporation having an address of 19000 Homestead Road, Cupertino, CA 95014. By signing this agreement, you are

agreeing to be bound by the terms of this agreement. If you refuse to sign this agreement you will be denied access to the network at the system administrator level.

Purpose

As a system administrator you will have access to company resources that are sensitive. With the privilege of system administrator access also comes a responsibility to the users, security manager, and others as deemed appropriate by Jamcracker. Adherence to the Jamcracker Administrative Security policy (in progress) is mandatory for all personnel granted this level of access. Any failure to comply with the Jamcracker policies will result in disciplinary action up to and including legal prosecution.

Termination

This agreement will remain in effect until Jamcracker or you have terminated your employment with Jamcracker, or you have been removed from the role as system administrator.

Conduct

You agree that at all times you shall conduct your system administrative duties in compliance with all applicable Jamcracker policies, federal and local laws and regulations, including, without limitation laws regulating your professional status and designation. The contents of electronic data, e.g. E-mail, will not be accessed or disclosed other than for security purposes or as required by law and only at the direction of the Security Manager. You further agree to the following:

- The system is to be maintained within the guidelines specified by the corporate Information Technology and Information Systems Security policies.
- No modifications to any system security policies, including logging will be made.
- The password on the local Administrator account will not change.
- The local Administrator account will not be disabled.
- Group membership on the system will not be modified.
- No operating systems or applications, which have not been authorized in accordance with the corporate policy, will be installed.

Agreement

I _____ fully understand my responsibilities and duties as a system administrator as defined by this agreement and the Jamcracker Inc. Security Policy. I shall conduct myself ethically and not abuse my position as system administrator. I understand that any violation of this agreement or any other company policies can be the basis for disciplinary action up to and including termination or judicial action.

_____ _____

Signature *Security Representative Signature*

Date: _____ Date: _____

Root User Access Security Policy Agreement

This is a legal agreement between you and Jamcracker, a Delaware corporation having an address of 19000 Homestead Road, Cupertino, CA 95014. By signing this agreement, you are agreeing to be bound by the terms of this agreement. If you refuse to sign this agreement you will be denied access to root user level of privileges.

Purpose

With root user privileges you will have access to system resources that are sensitive and use of the wrong commands could leave the system in an unusable state requiring a complete re-install of the OS and development work. With the privilege of root level access also comes a responsibility to the users, security manager, and others as deemed appropriate by Jamcracker. Adherence to the Jamcracker Administrative Security policy (in progress) is mandatory for all personnel granted this level of access. Any failure to comply with the Jamcracker policies will result in disciplinary action up to and including legal prosecution.

Termination

This agreement will remain in effect until Jamcracker or you have terminated your employment with Jamcracker, or you have been removed from the role as root user.

Conduct

You agree that at all times you shall conduct your root user duties in compliance with all applicable Jamcracker policies, federal and local laws and regulations, including, without limitation laws regulating your professional status and designation. The contents of electronic data, e.g. E-mail, will not be accessed or disclosed other than for security purposes or as required by law and only at the direction of the Security Manager. You further agree to the following:

- Direct root login access is not permitted, must "su – root" from a user account
- The system is to be maintained within the guidelines specified by the corporate Information Technology and Information Systems Security policies.
- System must not be left unattended with active root or user sessions active
- No modifications to any system security policies, including logging will be made.
- If the machine needs to be rebuilt, the logging facilities must be returned to original state
- The password on the local root account will not change.
- The password will not be given to anyone else.
- Group membership on the system will not be modified without approval.
- Applications that have not been authorized in accordance with the corporate policy, will not be installed.
- System name and IP address must not be changed without authorization
- Remote access to the servers must be via SSH or https, no clear text protocols can be used

Agreement

I _____ fully understand my responsibilities and duties using the root user account as defined by this agreement and the Jamcracker Inc. Security Policy. I shall conduct myself ethically and not abuse my root user privileges. I understand that any violation of this agreement or any other company policies can be the basis for disciplinary action up to and including termination or judicial action.

_____ _____

Signature *Security Representative Signature*

Date: _____ Date: _____

5.5. Appendix 5 – SFA Rules of Behavior

SFA needs to create.

5.6. Appendix 6 – Jamcracker Internet Usage Policy

See separate file.

5.7. Appendix 7– Personnel Termination Procedures

Purpose

This document defines the processes for termination of employment at Jamcracker, in the following two cases:

- The employee chooses to leave Jamcracker,
- Jamcracker chooses to terminate the employee.

Scope

This process applies to all employees who terminate their employment at Jamcracker, through either situation described above.

Roles & Responsibilities

- *Owner* – Human Resources (HR)
- *Who uses* – Direct managers of terminating employees, HR, Security, IO, Facilities

References

- JC-12-0027, *Corrective Action Procedure*
- JC-12-0085, *Deprovisioning Procedure*
- JC-14-0005, *Personnel Action Notice*
- JC-14-0012, *Exit Interview Checklist*

Revision History

Rev	*Release Date*	*Author*	*Approved by*	*Summary of changes*
A	08/22/00	G. Martin	G. Martin, K. Bomar, M. Ranganathan, L. Beavers, CJ Wickham, M. Siemon	Initial release
B	tbd	G. Martin		
C				

Definitions

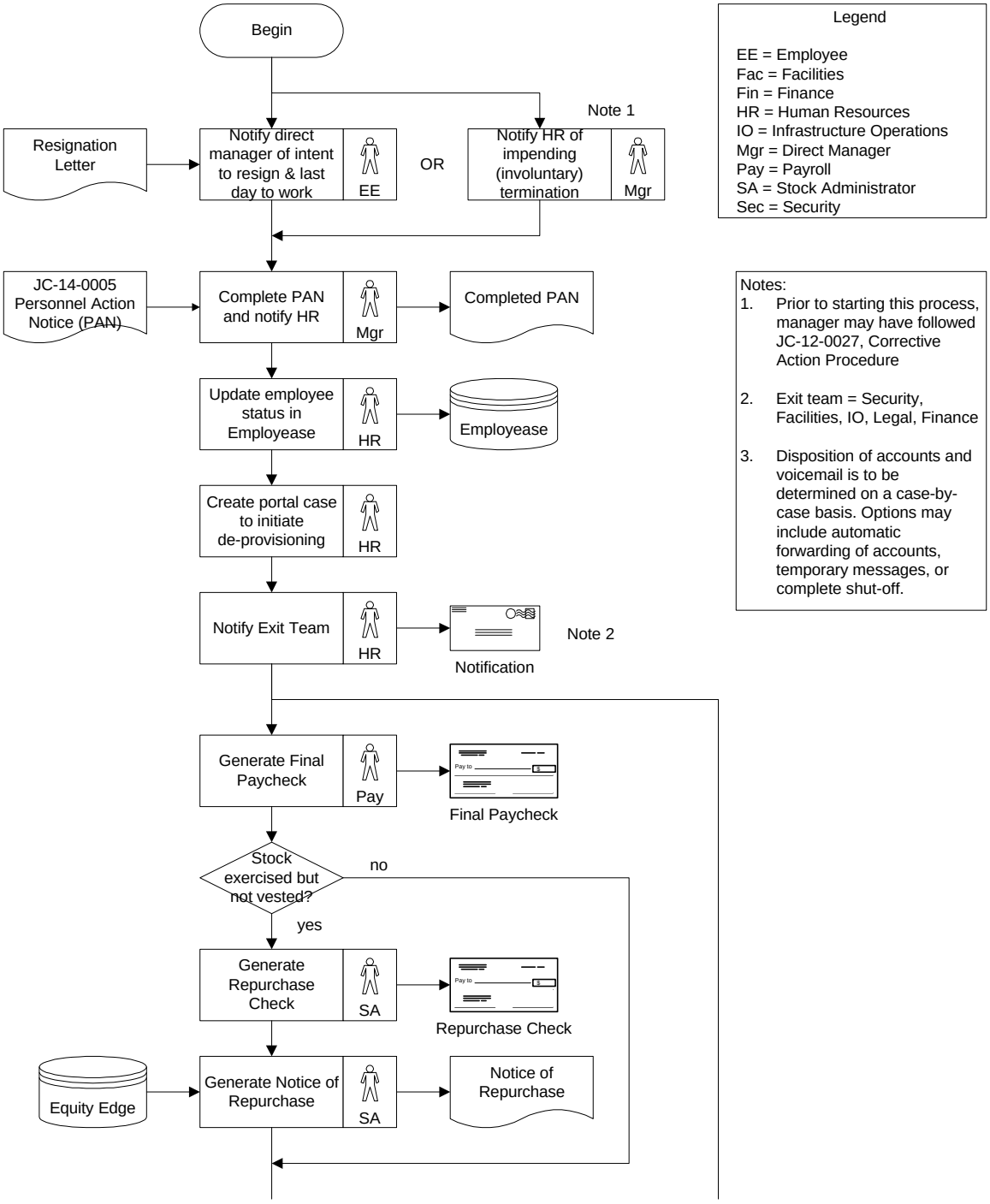
- *Voluntary* Termination: An employee chooses to leave his or her position at Jamcracker.
- *Involuntary* Termination: An employee is requested to leave his or her position at Jamcracker, based on a decision made by Jamcracker management.

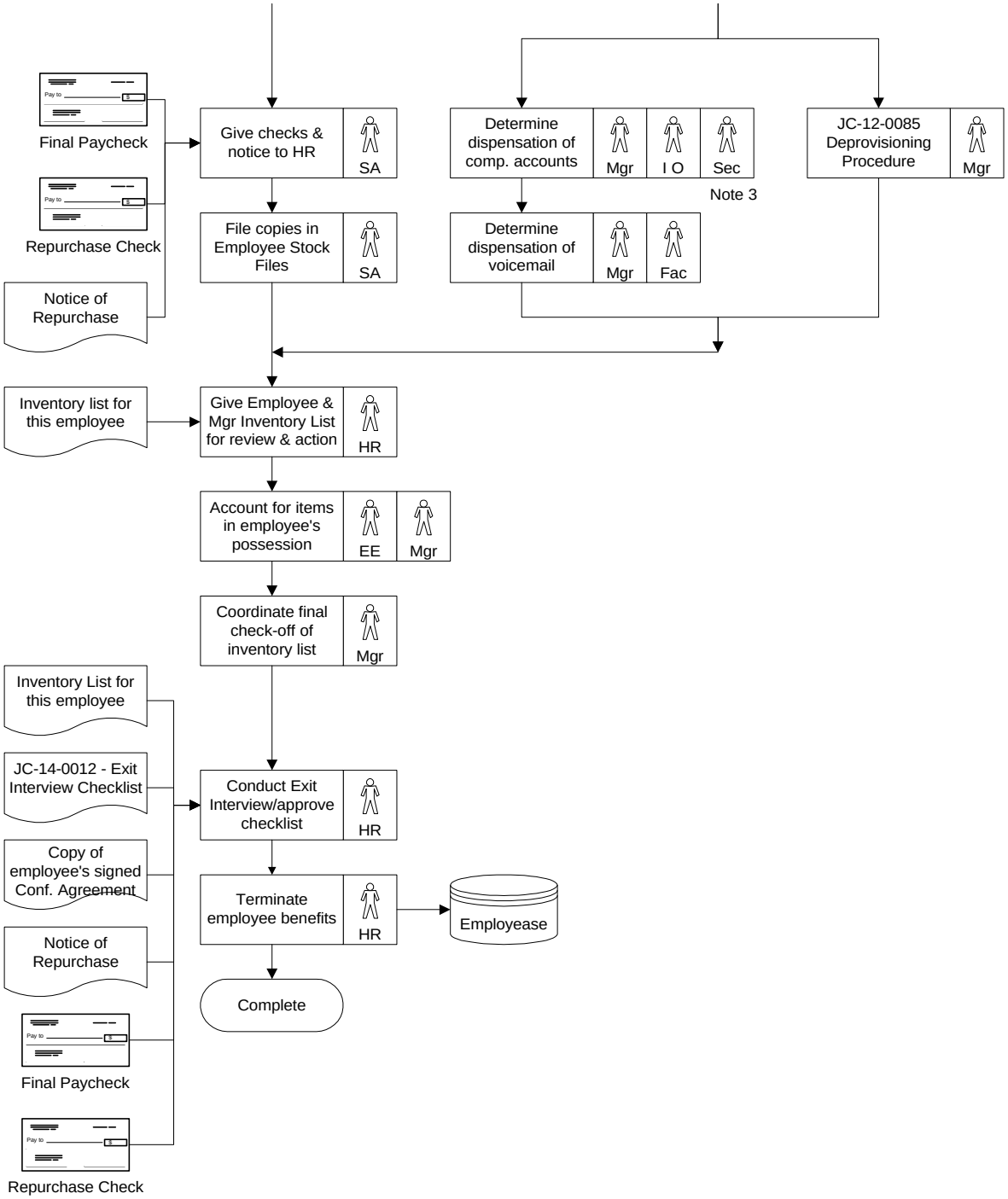
Results & Records

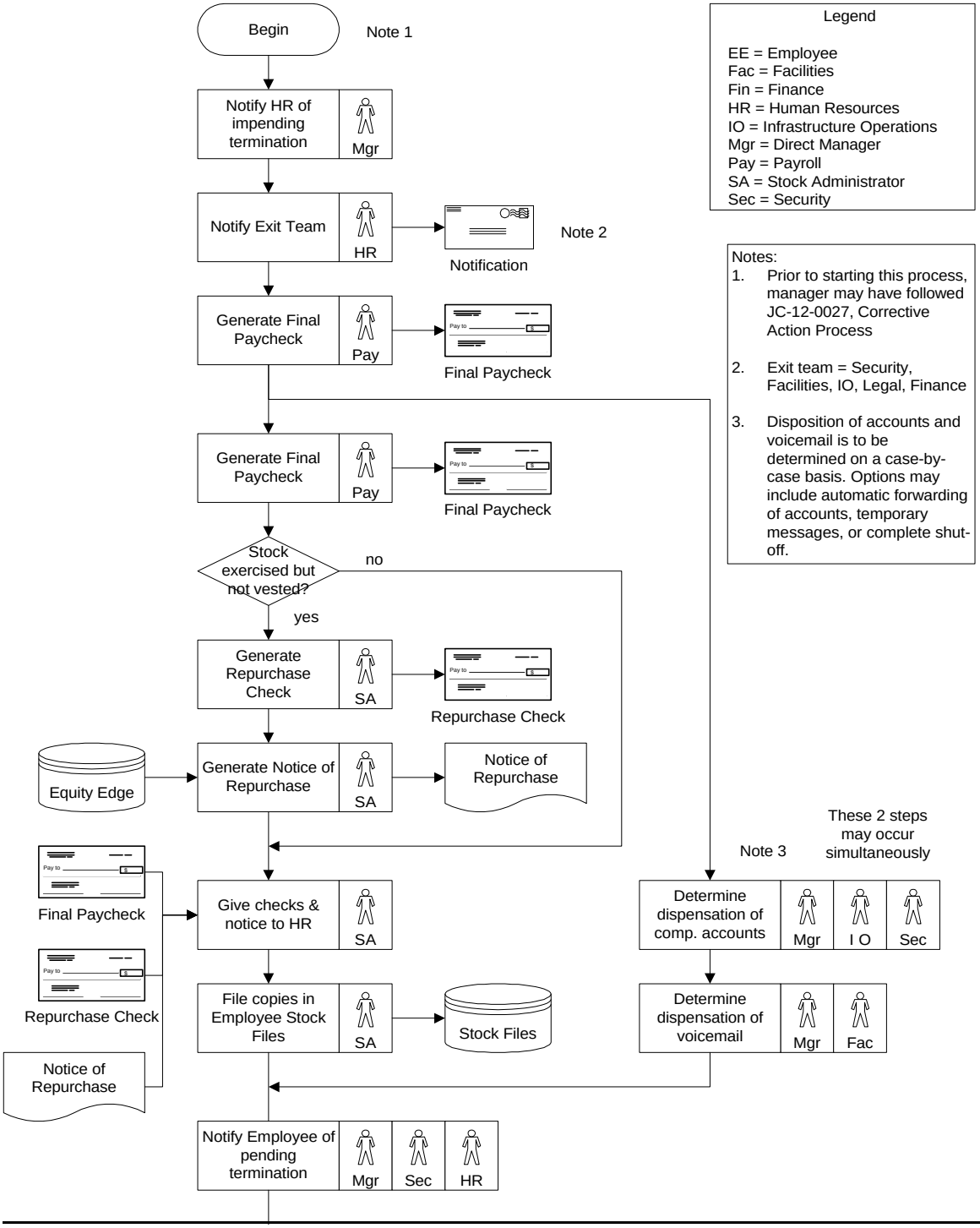
- Resignation letters are maintained in employee files.
- Exit Interview Checklists, and paperwork completed during the exit interview process, are maintained in employee files.

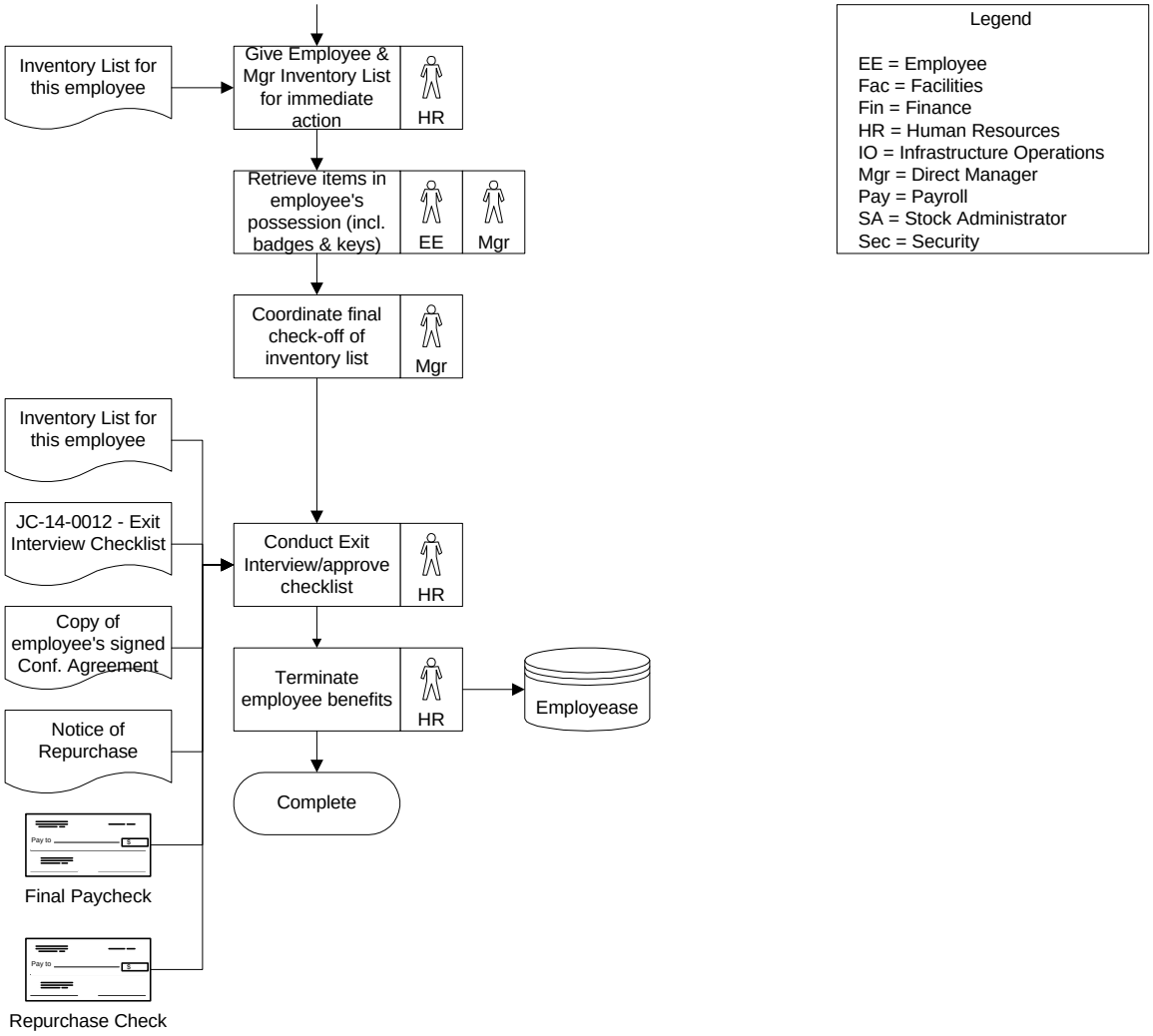
Flowcharts on the following pages:

1. Voluntary Termination
2. Involuntary Termination









5.8. Appendix 8 – Jamcracker Data Classification Guidelines

See separate file.

5.9. Appendix 9 – Jamcracker Guidelines for Encryption of Data

See separate file.

5.10. Appendix 10 – Jamcracker Pretty Good Privacy Usage Guidelines

See separate file.

5.11. Appendix 11 – Incident Response Procedures

Jamcracker Incident Response Procedures
(Draft Outline)

Responding to Intrusions

1. Establish policies and procedures for responding to intrusions.
2. Document configuration redundancy policy.
3. Document a response procedure that implements intrusion response policies.
4. Conduct a legal review of policies and procedures.
5. Train designated staff about response policies and procedures.

Prepare to respond to intrusions.

1. Build an archive of boot disks and distribution media for all applications and all operating systems and versions.
2. Build an archive of security-related patches for all applications and all operating systems and versions.
3. Identify and install tools that support the reinstallation of systems, applications, and patches.
4. Ensure that backup procedures are adequate to recover from any damage.
5. Build an archive of test results that describe the expected state of systems.
6. Ensure that high capacity, removable- and hardware-write-protectable media and supporting equipment are available to make and restore system backups.
7. Build and maintain a database of contact information.
8. Set up secure communication mechanisms.
9. Identify and install tools to access directories and other sources of contact information.
10. Build a resource kit of tools and hardware devices.

11. Ensure that test systems and networks are properly configured and available.

Analyze all available information to characterize an intrusion.

1. Capture and record system information that may be lost or not captured during the execution of backup procedure.
2. Backup the compromised systems.
3. "Isolate" the compromised systems.
4. Search on other systems for signs of intrusion.
5. Examine logs generated by firewalls, network monitors, and routers.
6. Identify the attacks used to gain access to systems.
7. Identify what an intruder did while accessing systems.

Communicate with all parties that need to be made aware of an intrusion and its progress.

1. Execute information dissemination procedures taking the specifics of an intrusion into account.
2. Use secure communication mechanisms.
3. Inform upstream and downstream sites of attacks and intrusions
4. Maintain a detailed contact log.
5. Maintain current contact information for systems and sites.

Collect and protect information associated with an intrusion.

1. Collect all information related to an intrusion.
2. Collect and preserve evidence.
3. Ensure evidence is captured and preserved securely.
4. Preserve the chain of custody for all evidence.
5. Contact law enforcement immediately if you decide to pursue and prosecute an intruder.

Apply short-term solutions to contain an intrusion.

1. Temporarily shut down the compromised system.
2. Disconnect the compromised system from a network.
3. Disable system services, if possible.
4. Change passwords or disable accounts.
5. Monitor system and network activities.
6. Verify that redundant systems and data have not been compromised.

Eliminate all means of intruder access.

1. Change all passwords on all systems to which the attacker may have had access.
2. Reinstall compromised systems if preparation was insufficient.

3. Remove any means for intruder access including changes made by an intruder.
4. Restore executable programs (including application services) and binary files from original distribution media.
5. Review system configurations.
6. Determine if you have uncorrected system and network vulnerabilities and correct them.
7. Improve protection mechanisms to limit the exposure of networks and systems.
8. Improve detection mechanisms to enable better reporting of attacks.

Return systems to normal operation.

1. Determine the requirements and timeframe for returning the system to normal operations.
2. Restore user data from trusted backup media.
3. Enable system and application services.
4. Reconnect the restored system to the network.
5. Validate the restored system.
6. Watch for additional scans or probes that may signal the return of an intruder.

Identify and implement security lessons learned.

1. If further notification is required (per policies and procedure), execute this notification.
2. Manage ongoing press aspects of an intrusion, if any.
3. Hold a post mortem analysis and review meeting with all involved parties.
4. Revise security plans, policies, procedures, and user and administrator training to prevent intrusion recurrence.
5. Determine whether or not to perform a new risk analysis based on the severity and impact of an intrusion.
6. Take a new inventory of system and network assets.
7. Participate in investigation and prosecution, if applicable.

5.12. Appendix 12 – Jamcracker Disaster Recovery Plan

The disaster recovery plan is a self-contained document--see separate file.

5.13. Appendix 13 – Data Integrity/Validation Controls

Data Integrity Policy Draft

Purpose

As the Jamcracker computing environment becomes more distributed, responsibility for the integrity of corporate and customer data that may reside on personal computers becomes distributed as well. The purpose of this policy is to identify the responsibilities of individual faculty and staff, departmental teams, and Technology Operations with respect to the protection of institutional machine-readable data.

Scope

This policy applies to all computerized corporate/customer data which resides on personal computers/microcomputers/servers. The policy addresses system data integrity in a distributed computing environment, specifically, the steps and measures to counter threats to data integrity.

Threats to Data Integrity

Several potential threats exist which can result in the corruption or loss of machine-readable data in a distributed computing environment. These threats can be classified in the general categories of hardware failure, user error, and system contamination.

Loss of data as a result of hardware failure is a byproduct of the fact that most microcomputers use magnetic media (i.e. floppy or hard disks) to store data. While this technology is generally quite reliable, data can be lost through either the gradual decomposition of the magnetic media itself or the failure of the mechanical components used to read and write data from the media. The media and mechanical components have a limited time of operational usefulness which can last as little as six months or up to several years. However, over a period of time, the media and the mechanical components will certainly fail, resulting in possible loss of data if adequate precautions are not taken.

The second potential threat to loss of data is attributable to user error. In most cases, individual microcomputer users have the ability to erase the entire contents of a magnetic disk. If a backup of the data that has been accidentally erased does not exist, it may be impossible to recover the data. Another method of protection from this threat is the use of input validation on critical fields within the Jamcracker Platform. All data fields that

are used in critical process functions are format specific. The user must enter the data in the required format or the data will not be accepted. Authorized customer users also have the ability to edit critical fields to keep user records up-to-date with changes in the customers organization.

The third potential threat to the loss of data can occur as a result of system contamination, usually caused by a computer virus. Computer viruses, of which several hundred "strains" have been identified, can be introduced into a system in a number of ways. In most cases, they are introduced when users exchange contaminated floppy diskettes between systems. Since most viruses are not immediately visible, it is very possible that one may exist for a significant period of time before being detected.

Jamcracker has implemented corporate wide anti-virus servers to monitor all critical servers for virus infection. These servers are maintained and monitored by the Jamcracker Security Operations Team and are updated via a “live update” service from the manufacturer. Incoming email is scanned for viruses by our external email service provider. This approach allows for redundancy in all virus scanning efforts and dramatically reduces the likelihood of infection by computer viruses.

The fourth potential threat to the loss of data can occur as a result of external intrusion or internal misuse of systems. Jamcracker limits remote access to its system to authorized Jamcracker customers and specific Jamcracker support staff. Threats from internal misuse are reduce by a separation of duties policy between departments and limiting users with “root” access privileges.

General Policies

In order to ensure the integrity of microcomputer-based data, individual computer users must assume primary responsibility for taking adequate precautions against loss of data. At the same time, this policy recognizes that supervisors, department heads, and the Technology Operations staff are responsible for ensuring that individual users have access to software and hardware necessary to ensure data integrity as well as adequate training in the use of these tools. Data that exist on microcomputers that were purchased with Jamcracker funds are considered to be corporate data. As such, individuals who are found to be negligent in maintaining the integrity of corporate data will be subject to appropriate corporate disciplinary actions. Individual employees will only be held responsible for loss of corporate data if reasonable steps were not taken to protect from such loss. These reasonable steps are outlined below.

General Responsibilities

Individual Employees/Users

Individual users bear the primary responsibility for the protection of data integrity in a distributed computing environment. As such, the following precautions should be taken by all Jamcracker employees who have corporate data stored on their computers:

a. Regular backups shall be maintained for all corporate data. In the case of floppy-disks, a duplicate copy of all disks shall be maintained. In the case of hard-disks, a backup copy shall be maintained on diskettes or tape. While users are encouraged to make incremental backups on a daily basis, this policy requires backups to be performed at least once weekly.
b. Users are responsible for taking reasonable steps to ensure they do not accidentally destroy corporate data. Users who are not proficient in the use of the application programs are required to enroll in appropriate training classes offered through the Educational Services Department in cooperation with the Technology Operations Team.
c. Users shall not copy data or programs from floppy disks onto their computer's disk(s) without taking reasonable steps to ensure that the diskette is not contaminated with a computer virus. For advice in this regard, users should consult with the Technology Operations team.

Department Heads/Supervisors

Department Heads and supervisory personnel also share in the responsibility for ensuring the integrity of corporate data. Under this policy, the responsibilities of supervisory personnel will include the following:

a. Department Heads and supervisors are responsible for ensuring that all employees for whom they are responsible have received adequate training in the use of microcomputer operating systems and applications.
b. Department Heads and supervisors are responsible for ensuring that legal copies of software necessary to perform backups of microcomputer disk drives is available to all employees for whom they have supervisory responsibility.

Jamcracker Technology Operations

The Technology Operations Team also has important responsibilities for ensuring the integrity of corporate data. Under this policy, the responsibilities of Technology Operations include the following:

a. The Technology Operations Team shall maintain a list of supported backup and anti-virus software and shall offer appropriate user support services for these products. This list shall be regularly updated in accordance with the Computing Resource Acquisition Policy.

b. The Technology Operations Team shall hold regular training classes on the management of microcomputer disks. This training shall include a discussion of strategies available to avoid data loss, including proper operating system command usage, backup strategies, and virus detection.

5.14. Appendix 14 – Jamcracker Platform Security Requirements

See separate file.

5.15. Appendix 15 – Guidelines for Secure Password Selection

See separate file.

5.16. Appendix 16 – Password Change Policy

Context

The primary purpose of this *Password change Policy* is to provide all required information about the procedures to follow to change the passwords of all systems that are critical. This policy highlights the steps to follow in changing system passwords in various circumstances.

The passwords are broadly classified into two main categories:
User passwords: used by the individuals to login to the network, operating systems, applications like e-mail, etc.
Service/System passwords: used by the systems to login to the other systems/services hosted internally and externally (ASPs)

All user passwords should be configurable so that it resets automatically after a pre-defined time.

The service/system passwords need to be reset manually by the systems personnel periodically and are classified as follows:

Internal systems:

- All the OS root passwords or admin passwords of all the production/ staging/development/QA servers or demo servers
- Database passwords (Oracle, LDAP, etc.)
- Application systems passwords/passphrases (Web servers, App servers, Clarify, BO, etc.)

External systems:

- ASP admin access passwords (SSO, Provisioning)
- Passwords that are used for automatic provisioning of users/services for the ASPs

This policy doesn't cover selecting the strong passwords, which is covered in **IT Security Policy**.

Policies

Persons who have special-privilege access to systems must be made aware of the Information Security issues that are directly related to passwords and implement the guidelines to minimize the risks.

The person/persons who manages the servers or systems are responsible for securing the passwords.

When any of the incidents explained in 2.2 occur, the proper method prescribed in the document should be followed, to ensure the safety and security of the Intellectual property of the company.

2.1 Change process and Procedure documents:

The people who deal with the passwords must maintain documents with detail processes for changing the passwords.

- This document should cover the impact of changing the passwords
- Dependencies or post effects in changing the passwords
- All the parties who should be notified when changing the passwords (like in the case of ASP passwords, the concerned Product Managers/Subject matter experts)

The people who make changes to passwords should clearly document in "Change Management Systems" the details of when and what the changes being made are.

2.2 When should you change passwords?

- All the critical passwords should be changed periodically, at least once every three months. In the case of production system passwords, the change should take place during the maintenance window; if there is no scheduled maintenance

window, one should schedule it and follow the same process of any maintenance window.

- All Systems Admin, Database Admin, Network Admin, CSR/TSR, TAM. SME, Product Managers are privileged users. Each privileged user might know at least one or more passwords. When any of the privileged users leave the company, change the password immediately. Some designated users are authorized to call vendor-specific tech support.
- Some times passwords may need to be shared with system support personnel for troubleshooting purposes; in those cases, the passwords should be changed immediately after the troubleshooting is over.
- Change all passwords immediately after any known incidents of system compromise.

2.3 Who changes the passwords?

Whoever owns/is responsible for maintaining the systems should change the passwords.

- In the case of production systems, I/O personnel should change them. The changed passwords should not be shared with others.
- In the case of server passwords, the Sys Admin should identify and change all the root and pseudo root passwords. The Sys Admins should periodically audit the systems for any unauthorized pseudo accounts. If they find any they should immediately disable those accounts.
- Product Managers should take the active role in changing the ASP related passwords. They should coordinate with the ASP contact person and change the passwords so the downtime to the end-customers will be minimized.

2.4 Guidelines in changing passwords:

Before changing any passwords, all the involved parties should be notified in advance. In the case of ASP partner passwords, the change request should go through the concerned Product Manager (PM). The PM should coordinate with the ASP partner contact. All PMs should maintain the contact information for primary and secondary ASP partner contacts. This should be made available to the secondary person on his/her team. If possible, password changes should be tested with the Staging environment to avoid any kind of outage in production.

The passwords should be made different on production systems versus non-production systems.

One should remember to select the strong password scheme when changing passwords.

5.17. Appendix 17 – Audit Trails

Portal Workspace Auditing Functions

Security auditing involves recognizing, recording, storing, and analyzing information related to security relevant activities (i.e., activities controlled by the security policy). The resulting audit records can be examined to determine which security relevant activities took place and which user is responsible for them.

Security audit automatic response

Overview

This function defines the response to be taken in case of detected events indicative of a potential security violation.

Management

- the management (addition, removal, or modification) of actions.

Requirements

The following actions should be auditable:

- Minimal: Actions taken due to imminent security violations.

Security audit data generation

Overview

This function defines requirements for recording the occurrence of security relevant events that take place. This function also identifies the level of auditing, enumerates the types of events that shall be auditable by the workspace, and identifies the minimum set of audit-related information that should be provided within various audit record types. Audit data generation defines the level of auditable events, and specifies the list of data that shall be recorded in each record. User identity association, the workspace shall associate auditable events to individual user identities.

Requirements

The following actions should be auditable:

- Start-up and shutdown of the audit functions

- All auditable events for the [selection: *minimum, basic, detailed, not specifie*d] level of audit
- Log any administrative changes (for example, any change to admin roles)
- Any password resets
- Change Username
- Change Company Name
- Add/Modify/Suspend/Delete Company
- Add/Modify/Suspend/Delete User
- Add/Modify/Suspend/Delete Service for Company
- Add/Modify/Suspend/Delete Service for User
- Modify User Role
- [Assignment: other specifically defined auditable events].

The workspace shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the security policy, [assignment: *other audit relevant informatio*n]

Security audit analysis

Overview

This function defines requirements for automated means that analysis system activity and audit data looking for possible or real security violations. This analysis may work in support of intrusion detection, or automatic response to an imminent security violation.

Management

- Maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules.
- Maintenance (deletion, modification, addition) of the group of users in the profile target group.
- Maintenance (deletion, modification, addition) of the subset of system events.
- Maintenance (deletion, modification, addition) of the set of sequence of system events.

Behavior Overview

Potential violation analysis, basic threshold detection on the basis of a fixed rule set is required.

Behavior 1:

Profile based anomaly detection; the workspace maintains individual *profiles* of system usage, where a profile represents the historical patterns of usage performed by members of the *profile target group*. A profile target group refers to a group of one or more individuals (e.g., a single user, users who share a group ID or group account, users who operate under an assigned role, users of an entire system or network node) who interact with the workspace. Each member of a profile target group is assigned an individual *suspicion rating* that represents how well that member's current activity corresponds to the established patterns of usage represented in the profile. This analysis can be performed at runtime or during a post-collection batch-mode analysis.

Management

- Minimal: Enabling and disabling of any of the analysis mechanisms;
- Minimal: Automated responses performed by the tool.

Behavior 2:

Simple attack heuristics, the workspace shall be able to detect the occurrence of signature events that represent a significant threat to security policy enforcement. This search for signature events may occur in real-time or during a post-collection batch-mode analysis.

Management

- Minimal: Enabling and disabling of any of the analysis mechanisms;
- Minimal: Automated responses performed by the tool.

Behavior 3:

Complex attack heuristics, the workspace shall be able to represent and detect multi-step intrusion scenarios. The workspace is able to compare system events (possibly performed by multiple individuals) against event sequences known to represent entire intrusion scenarios. The workspace shall be able to indicate when a signature event or event sequence is found that indicates a potential violation of the security policy.

Management

- Minimal: Enabling and disabling of any of the analysis mechanisms;

- Minimal: Automated responses performed by the tool.

Requirements

Security audit review

Overview

This function defines the requirements for audit tools that should be available to authorized users to assist in the review of audit data.

Management

The following actions could be considered for the management functions in audit review:

- Maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.

Requirements

- The workspace shall provide [assignment: *authorized user*s] with the capability to read [assignment: *list of audit informatio*n] from the audit records.
- The workspace shall provide the audit records in a manner suitable for the user to interpret the information.
- The workspace shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.
- The workspace shall provide the ability to perform [selection: searches, sorting, ordering] of audit data based on [assignment: criteria with logical relations].

This component will provide authorized users the capability to obtain and interpret the information. In case of human users this information needs to be in a human understandable presentation. In case of external IT entities the information needs to be unambiguously represented in an electronic fashion.

Security audit event selection

Overview

This function defines requirements to select the events to be audited during workspace operation. It defines requirements to include or exclude events from

the set of auditable events. Selective audit requires the ability to include or exclude events from the set of audited events based upon attributes to be specified by the security policy author.

Management

The following actions could be considered for the management functions for audit event selection:

- Maintenance of the rights to view/modify the audit events.

Requirements

The workspace shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

- [Selection: object identity, user identity, subject identity, host identity, and event type]
- [Assignment: list of additional attributes that audit selectivity is based upon].

Security audit event storage

Overview

This function defines the requirements for the workspace to be able to create and maintain a secure audit trail.

Requirement 1

Protected audit trail storage, requirements are placed on the audit trail. It will be protected from unauthorized deletion and/or modification.

Management

There are no management activities foreseen

Requirement 2

Action in case of possible audit data loss specifies actions to be taken if a threshold on the audit trail is exceeded.

Management

- Maintenance of the threshold;
- Maintenance (deletion, modification, addition) of actions to be taken in case of imminent audit storage failure.

Requirement 3

Prevention of audit data loss specifies actions in case the audit trail is full.

Management

- Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.

5.18. Appendix 18 – Jamcracker Acceptable Usage Guidelines

See separate file.

5.19. Appendix 19 – HR Mod SSO Assignment Letter

SFA needs to create.

5.20. Appendix 20 – JC-12-0043 Change Administration & Rollout Management Manual

See separate file.

5.21. Appendix 21 – HR Mod Users and Roles

Type of User	Functionality
SFA Employee	Update user profile; select members of user group; delete members of user group except Manager; change Manager selection; create goals; edit goals; view goals; archive goals; distribute goals; update goal progress; establish appraisal form; edit appraisal form; complete appraisal form; view appraisal form; print appraisal form; create development note; edit draft development note; delete draft development note; view completed development note; archive development note; view development note; view and print goal statistics report, goal summary report, progress history report, and development notes report.
SFA Manager	Same functionality as SFA Employee plus: view subordinate's goal; approve subordinate's goal; decline subordinate's goal; approve subordinate's appraisal form; decline subordinate's appraisal form; view subordinate's development note; view and print subordinate's goals statistics report, goal summary report, progress history report, and development notes report.
System Administrator	Same functionality as SFA Employee and SFA Manager plus: set default access type; set default language; set default password for new users; allow users to update their EEO status, gender, date of birth; allow users to update their organization, sets who must approve a change in an

	employee's organization; allow users to update their final approver and direct manager; sets who must approve a change in an employee's user group; view details of any user including general information and contact information; change employee's password; create new user; edit relationships; create new relationships; make relationship active or inactive; view or edit existing entity; create new entity; view or edit existing access type; create new access type; view or edit existing rating scale; create new rating scale; view or edit existing category; create new category; approve addition or deletion to employees' user groups; approve organization selection changes; approve changes to Direct Manager or Final Approver; set whether require employees to approve draft appraisal forms; set whether require employees to sign off on final appraisals; set whether require Final Approver to approve review copies; set whether require ratings for all criteria including goals and open criteria; set whether require overall appraisal rating scale on all appraisals; set default rating scale for goals; set default rating scale for open criteria; set whether comments for all ratings; set whether require Primary Rater to be Direct Manager; set whether allow Primary Rater to edit consolidated ratings; select who is allowed to view and assess goals; set number of recommended relationships; view or edit existing period; create new period; delete period; set whether Primary Rater is notified when a goal status is changed; set whether level descriptions are required for all weight levels; set whether supervisor can view subordinates' goals and not vice versa; set whether joint approval status is required for goals; set whether you have an update day for updating goal progress; set default update day; select a primary category and secondary category for grouping; view or edit existing weighting scales by changing level descriptions, weight values, select default weight and determine which goals are fed into the Appraisal module; view or edit existing unit of measure; select default unit of measure; create new unit of measure; select default rating scale to be used when creating new competencies; select primary and secondary category for grouping competencies on appraisal forms; view or edit existing competencies; create new competency; view, edit, or

	delete existing profiles; create new competency profile such as CIO Employee or CIO Manager.